UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/735,570	12/12/2000	Raymond Lin	AGIL-0200	5738

7590 01/04/2005

David R. Stevens
Stevens & Westberg LLP
99 North First Street, Suite 201
San Jose, CA 95113

EXAMINER	
PATEL, ASHOKKUMAR B	

ART UNIT	PAPER NUMBER
2154	

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/735,570	LIN ET AL.	
	Examiner	Art Unit	
	Ashok B. Patel	2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 October 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,11-19 and 21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,11-19 and 21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Application Number 09/735,570 was filed on 12/12/2000. Claims 1-22 are subject to examination. Claims 9, 10 and 22 have been cancelled. Claim 20 does not exist.

Response to Arguments

2. Applicant's arguments with respect to claims 1-22 have been considered but are moot in view of the new ground(s) of rejection.

Specification

3. Claim 2 is objected to because of the following informalities: In line 3, the claim recites " to privileges associated with a browser prevent an....." It should read "to privileges associated with a browser to prevent an ....." Appropriate correction is required.

4. Claim 4 is objected to because of the following informalities: In line 2, the claim recites " a monitoring thread from for facilitating....." It should read "a monitoring thread for facilitating ....." Appropriate correction is required.

5. The amendment filed October 01, 2004 is objected to under 35 U.S.C. 132 because it introduces new matter into the disclosure. 35 U.S.C. 132 states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: In claim 2, wherein it recites "a browser prevent an unauthorized attack from multiple browser requests that may shut down an application server if the browser requests were allowed direct access.

Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-8, 11-19 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bandhole et al. (hereinafter Bandhole) (US 2002/0049803 A1) in view of Lin et al. (hereinafter Lin) (US 6, 751, 668 B1)

Referring to claim 1,

The reference Bandhole teaches a system for facilitating communication between a web browser and an application server via an intermediate webserver and for preventing unauthorized attacks of browser attacks directed to an application server (Figs 2 and 3), comprising:

a webserver (Fig.3, element 309) configured to communicate with a network (Fig.3, element 307) and maintain information related to the authorization of browser requests directed to an application server (page 6, para. [0049]) , the webserver having an application server interface (Fig.3, element 309) for communicating with an application server (Fig.3, element 342)and a network interface for communicating with entities via a network (Fig.3, element 307);

a state server configured to store data related to communication sessions occurring among a web browser, a webserver and an application server, the state server including a communication interface configured to communicate with the webserver (Fig.3, element 331, note: page 6, para. [0052], Note: "That is, each of the managers need not reside in a single application server 311, but rather might be operably disposed over two or more machines.");

wherein the application server interface (Fig. 3, element 309) is configured to communicate with an application server (Fig. 3, element 309), the application server interface including a mechanism for receiving a signal from an application server indicating an authorization to communicate with the application server (page 6, para. 0056], Note: "That is, each of the managers need not reside in a single application server 311, but rather might be operably disposed over two or more machines.") , the application server interface further configured to monitor the session between an application server and a browser (page 6, para. 0056], Note: "Accounts manager 329, which is sometimes referred to as a user manager, is configured to communicate with the session manager 331 and operates to create, maintain and remove all user account information specific to each user at one or more clients 301. Such information includes the login name, password, user name, email address and the authorized activities for each of the users."); and

a load balancing device configured to receive browser requests among a plurality of webservers, wherein the load balancing device is further configured to screen the browser requests according to predetermined criteria including preauthorization indicia,

wherein browser requests are prevented from making an unfriendly attack to the system. (Fig.2, element 219, note: switch tier includes fire wall and load balancer)

Although, the reference Bandhole teaches in page 6, para. [0049]) "The connection between client 301 and web server 309 may either be, for example, a secure or an insecure connection. For instance, the connection may use the Secure Socket Layer (SSL) protocol to ensure security of the data transmission between client 301 and web server 309.", the reference fails to teach "browser requests to prevent multiple unauthorized browser attacks directed to an application server". The reference Lin teaches "A filter 106 operates to selectively block session establishment packets 108 from being provided to the target 104. In particular, an abnormally high number of session establishment attempts is usually an indication that a denial of service (DoS) attack is occurring. The filter 106 records the total number of existing sessions and measures the rate of session requests of each stream. A "stream" is a data traffic flow between a particular source and a specific target.", col. 2, lines 10-16. As it is evident from the depiction of the Lin's filter in Fig. 1, the filter itself affords its implementation anywhere in a given system.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to enhance Bandhole's webserver and its account manager, Fig.3, element 329 (the application server interface) by adding Lin's filter such that the denial of service attacks can be handled without entirely blocking all new session connection requests. Again, this would have been obvious because it allows rather than denying all new session requests or denying no new session requests (and,

albeit, dropping then-pending session requests), new session requests are selectively passed to the device.

Referring to claim 2,

The reference Bandhole teaches a system according to Claim 1, wherein the application server interface (Fig. 3, element 329, page 6, para. 0056], Note: "That is, each of the managers need not reside in a single application server 311, but rather might be operably disposed over two or more machines.") is configured to communicate with an application server only when a signal is received by the webserver that authorizes such communication according to privileges associated with a browser. (page 6, para.[0056], "Such information includes the login name, password, user name, email address and the authorized activities for each of the users.")

Although, the reference Bandhole teaches in page 6, para. [0049]) "The connection between client 301 and web server 309 may either be, for example, a secure or an insecure connection. For instance, the connection may use the Secure Socket Layer (SSL) protocol to ensure security of the data transmission between client 301 and web server 309.", the reference fails to teach "browser requests to prevent multiple unauthorized browser attacks directed to an application server". The reference Lin teaches "A filter 106 operates to selectively block session establishment packets 108 from being provided to the target 104. In particular, an abnormally high number of session establishment attempts is usually an indication that a denial of service (DoS) attack is occurring. The filter 106 records the total number of existing sessions and measures the rate of session requests of each stream. A "stream" is a data traffic flow

between a particular source and a specific target.", col. 2, lines 10-16. As it is evident from the depiction of the Lin's filter in Fig. 1, the filter itself affords its implementation anywhere in a given system.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to enhance Bandhole's webserver and its account manager, Fig.3, element 329 (the application server interface) by adding Lin's filter such that the denial of service attacks can be handled without entirely blocking all new session connection requests. Again, this would have been obvious because it allows rather than denying all new session requests or denying no new session requests (and, albeit, dropping then-pending session requests), new session requests are selectively passed to the device.

Referring to claim 3,

The reference Bandhole teaches a system according to Claim 2, wherein the application server interface includes a monitoring mechanism for monitoring the activity of the application server during a session with a browser and a screening mechanism configured to prevent access to browser requests that are not authorized to access an application server according to predetermined privileges. (page 6, para. [0056])

Referring to claim 4,

The reference Bandhole teaches a system according to Claim 2, wherein the application server interface includes a monitoring thread for facilitating the monitoring by the webserver of the activity of the application server during a session with a browser (page 6, para. [0056]). the state server configured to define privileges associated with a

browser request that define the parameters in which a browser may access an application server. (page 6, para. [0055], note: "For example, a session manager 331 coordinates information related to the user, the capabilities of the user, machine configurations associated with the user's account, as well as commands to open windows on machines or to shut down machines")

Referring to claim 5,

The reference Bandhole teaches a system according to Claim 2, wherein the application server interface is further configured to receive a monitoring thread from an application server so that the webserver can monitor the activities of a application server during a session between the application server and a browser (page 6, para. [0056]), the state server configured to define privileges associated with a browser request that define the parameters in which a browser may access art application server including limits to predefined information or services. (page 6, para. [0055], note: "For example, a session manager 331 coordinates information related to the user, the capabilities of the user, machine configurations associated with the user's account, as well as commands to open windows on machines or to shut down machines")

Referring to claim 6,

The reference Bandhole teaches a system according to Claim 2, wherein the application server interface is further configured with a monitoring mechanism that allows any application server to monitor the activities of a webserver during a session between the application server and a browser (page 6, para. [0056]), the state server configured to define-privileges associated with a browser request that define the parameters in which

a browser may access an. application server including predetermined commands a browser may send to the application server (page 6, para. [0055], note: "For example, a session manager 331 coordinates information related to the user, the capabilities of the user, machine configurations associated with the user's account, as well as commands to open windows on machines or to shut down machines.") Although, the reference Bandhole teaches in page 6, para. [0049]) "The connection between client 301 and web server 309 may either be, for example, a secure or an insecure connection. For instance, the connection may use the Secure Socket Layer (SSL) protocol to ensure security of the data transmission between client 301 and web server 309.", the reference fails to teach "indicative of an unauthorized attack by multiple browser commands". The reference Lin teaches "A filter 106 operates to selectively block session establishment packets 108 from being provided to the target 104. In particular, an abnormally high number of session establishment attempts is usually an indication that a denial of service (DoS) attack is occurring. The filter 106 records the total number of existing sessions and measures the rate of session requests of each stream. A "stream" is a data traffic flow between a particular source and a specific target.", col. 2, lines 10-16 (indicative of an unauthorized attack by multiple browser commands.). As it is evident from the depiction of the Lin's filter in Fig. 1, the filter itself affords its implementation anywhere in a given system. Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to enhance Bandhole's webserver and its account manager, Fig.3, element 329 (the application server interface) by adding Lin's filter such that the denial of service attacks can be

handled without entirely blocking all new session connection requests. Again, this would have been obvious because it allows rather than denying all new session requests or denying no new session requests (and, albeit, dropping then-pending session requests), new session requests are selectively passed to the device.

Referring to claim 7,

The reference Bandhole teaches a system according to Claim 2, wherein the application server interface is further configured to receive a monitoring thread front an application server so that an application server can monitor the activities of a webserver during a session between the application server and a browser (page 6, para. [0056]), the state server configured to define privileges associated with a browser request that define predetermined commands a browser may send to the application server (page 6, para. [0055], note: "For example, a session manager 331 coordinates information related to the user, the capabilities of the user, machine configurations associated with the user's account, as well as commands to open windows on machines or to shut down machines.") Although, the reference Bandhole teaches in page 6, para. [0049]) "The connection between client 301 and web server 309 may either be, for example, a secure or an insecure connection. For instance, the connection may use the Secure Socket Layer (SSL) protocol to ensure security of the data transmission between client 301 and web server 309.", the reference fails to teach "indicative of an unauthorized attack by multiple browser commands". The reference Lin teaches "A filter 106 operates to selectively block session establishment packets 108 from being provided to the target 104. In particular, an abnormally high number of session establishment

attempts is usually an indication that a denial of service (DoS) attack is occurring. The filter 106 records the total number of existing sessions and measures the rate of session requests of each stream. A "stream" is a data traffic flow between a particular source and a specific target.", col. 2, lines 10-16 (indicative of an unauthorized attack by multiple browser commands.). As it is evident from the depiction of the Lin's filter in Fig. 1, the filter itself affords its implementation anywhere in a given system. Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to enhance Bandhole's webserver and its account manager, Fig.3, element 329 (the application server interface) by adding Lin's filter such that the denial of service attacks can be handled without entirely blocking all new session connection requests. Again, this would have been obvious because it allows rather than denying all new session requests or denying no new session requests (and, albeit, dropping then-pending session requests), new session requests are selectively passed to the device.

Referring to claim 8,

The reference Bandhole teaches a system according to Claim 2, further comprising a second webserver communicating with the other webserver and with the state server, wherein the second webserver is further configured to take over a session occurring between the application server and a browser being monitored by the other webserver in the event the other webserver stops monitoring the session that is associated with a browser request that has been screened and authorized to access an application server. (page 5, para. [0042] and [0043])

Referring to claim 11,

The reference Bandhole teaches a system fox communicating among a plurality of network servers communicating with a plurality of computers arid for preventing unauthorized attacks of browser attacks directed to an application server (Figs. 2 and 3), comprising:

a plurality of webservers communicating with and configured to receive a request from a web browser (Fig. 2, elements 205) and to screen and route the browser request to an application server upon the receipt of a signal from the application server (page 6, para. 0056], Note: "That is, each of the managers need not reside in a single application server 311, but rather might be operably disposed over two or more machines.", "Accounts manager 329, which is sometimes referred to as a user manager, is configured to communicate with the session manager 331 and operates to create, maintain and remove all user account information specific to each user at one or more clients 301. Such information includes the login name, password, user name, email address and the authorized activities for each of the users."), wherein each webserver is configured to maintain information related to the authorization of browser requests (page 6, para.[0049]);

an application server interface configured to control communication between the plurality of webservers and an application server (page 6, para. 0056], Note: "Accounts manager 329, which is sometimes referred to as a user manager, is configured to communicate with the session manager 331 and operates to create, maintain and remove all user account information specific to each user at one or more clients 301.

Such information includes the login name, password, user name, email address and the authorized activities for each of the users.");

a state server configured to store data related to communication sessions occurring among a web browser, a webserver and an application server, wherein a first webserver is configured to retrieve information related to a session between a web browser and an application server and being monitored by a second webserver in the event that the second webserver terminates its monitoring of the session (Fig.3, element 331, note: page 6, para. [0052], Note: "That is, each of the managers need not reside in a single application server 311, but rather might be operably disposed over two or more machines."), page 5, para. [0042] and [0043]); and

a load balancing device configured to receive browser requests among a plurality of webservers, wherein the load balancing device is further configured to screen the browser requests according to predetermined criteria including „preauthorization indicia, wherein browser requests are prevented from making an unfriendly attack to the system. (Fig.2, element 219, note: switch tier includes fire wall and load balancer).

Although, the reference Bandhole teaches in page 6, para. [0049]) "The connection between client 301 and web server 309 may either be, for example, a secure or an insecure connection. For instance, the connection may use the Secure Socket Layer (SSL) protocol to ensure security of the data transmission between client 301 and web server 309.", the reference fails to teach "browser requests to prevent multiple unauthorized browser attacks directed to an application server". The reference Lin teaches "A filter 106 operates to selectively block session establishment packets

108 from being provided to the target 104. In particular, an abnormally high number of session establishment attempts is usually an indication that a denial of service (DoS) attack is occurring. The filter 106 records the total number of existing sessions and measures the rate of session requests of each stream. A "stream" is a data traffic flow between a particular source and a specific target.", col. 2, lines 10-16. As it is evident from the depiction of the Lin's filter in Fig. 1, the filter itself affords its implementation anywhere in a given system.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to enhance Bandhole's webserver and its account manager, Fig.3, element 329 (the application server interface) by adding Lin's filter such that the denial of service attacks can be handled without entirely blocking all new session connection requests. Again, this would have been obvious because it allows rather than denying all new session requests or denying no new session requests (and, albeit, dropping then-pending session requests), new session requests are selectively passed to the device.

Referring to claim 12,

The reference Bandhole teaches a system according to Claim 11 further comprising a database communicating with the state server and configured to store session information and for storing and maintaining browser request privileges that define whether a browser is authorized to access an application server to prevent direct attacks of browser attacks on application severs. (Fig. 3, element 350 and page 6,

para.[0055], "the session manager 311 monitors and archives the activities of each of the users at client 301 for any given session.")

Referring to claim 13,

The reference Bandhole teaches a system according to Claim 11, wherein the webserver is configured to route a browser request to an application server only upon the receipt of a signal from the application server indicating that the application server is ready to receive browser requests (page 6, para. [0056]) and wherein the state server is configured for storing and maintaining browser request privileges that define whether a browser is authorized to access an application server. (Fig. 3, element 331, page 6, para. [0056]). Although, the reference Bandhole teaches in page 6, para. [0049]) "The connection between client 301 and web server 309 may either be, for example, a secure or an insecure connection. For instance, the connection may use the Secure Socket Layer (SSL) protocol to ensure security of the data transmission between client 301 and web server 309.", the reference fails to teach "to prevent direct attacks of browser attacks on application servers". The reference Lin teaches "A filter 106 operates to selectively block session establishment packets 108 from being provided to the target 104. In particular, an abnormally high number of session establishment attempts is usually an indication that a denial of service (DoS) attack is occurring. The filter 106 records the total number of existing sessions and measures the rate of session requests of each stream. A "stream" is a data traffic flow between a particular source and a specific target.", col. 2, lines 10-16 ("to prevent direct attacks of browser attacks on application servers"). As it is evident from the depiction of the Lin's filter in Fig. 1, the

filter itself affords its implementation anywhere in a given system. Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to enhance Bandhole's webserver and its account manager, Fig.3, element 329 (the application server interface) by adding Lin's filter such that the denial of service attacks can be handled without entirely blocking all new session connection requests. Again, this would have been obvious because it allows rather than denying all new session requests or denying no new session requests (and, albeit, dropping then-pending session requests), new session requests are selectively passed to the device.

Referring to claim 14,

The reference teaches Bandhole teaches a system according to Claim 11 further comprising a load balancing device configured to receive browser requests sent from computers communicating with the network system and to direct the requests among the plurality of application servers (Fig.2, elements 219 and 207), wherein the state server is configured for storing and maintaining browser request privileges that define whether a browser is authorized to access an application server (Fig. 3, element 331, page 6, para. [0056]). Although, the reference Bandhole teaches in page 6, para. [0049]) "The connection between client 301 and web server 309 may either be, for example, a secure or an insecure connection. For instance, the connection may use the Secure Socket Layer (SSL) protocol to ensure security of the data transmission between client 301 and web server 309.", the reference fails to teach "to prevent direct attacks of browser attacks on application servers". The reference Lin teaches "A filter 106 operates to selectively block session establishment packets 108 from being

provided to the target 104. In particular, an abnormally high number of session establishment attempts is usually an indication that a denial of service (DoS) attack is occurring. The filter 106 records the total number of existing sessions and measures the rate of session requests of each stream. A "stream" is a data traffic flow between a particular source and a specific target.", col. 2, lines 10-16 ("to prevent direct attacks of browser attacks on application servers"). As it is evident from the depiction of the Lin's filter in Fig. 1, the filter itself affords its implementation anywhere in a given system. Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to enhance Bandhole's webserver and its account manager, Fig.3, element 329 (the application server interface) by adding Lin's filter such that the denial of service attacks can be handled without entirely blocking all new session connection requests. Again, this would have been obvious because it allows rather than denying all new session requests or denying no new session requests (and, albeit, dropping then-pending session requests), new session requests are selectively passed to the device.

Referring to claim 15,

The reference Bandhole teaches a method of facilitating communication between a web browser and an application server (Figs. 2 and 3) , comprising:

receiving a request for access to an application server;

receiving the request by a first webserver (page 6, para.[0048] and [0049]);

screening the request for determining authority to access the application server by accessing the state server to determine whether a browser is authorized to access

an application server to prevent attacks by multiple browser requests (page 6, para.[0056]);

receiving a signal from the application server indicating that it is ready to receive a browser request; communicating with the application server to create a monitoring thread between the webserver and the application server; and if the browser request is screened and authorized to access the application server, facilitating communication between the browser and the application server with the webserver. (page 6, para. [0054]-[0056])

Referring to claim 16,

The reference Bandhole teaches a method according to Claim 15, further comprising: communicating with a state server to create a monitoring mechanism between the webserver and the state server to monitor communications between a web browser and an application server (Fig 3, elements 329 and 331) and to store information related to such communications and to store privilege information associated with browser requests (Fig. 3, element 350 and page 6, Para. [0055], "the session manager 311 monitors and archives the activities of each of the users at client 301 for any given session.") Although, the reference Bandhole teaches in page 6, para. [0049]) "The connection between client 301 and web server 309 may either be, for example, a secure or an insecure connection. For instance, the connection may use the Secure Socket Layer (SSL) protocol to ensure security of the data transmission between client 301 and web server 309.", the reference fails to teach "to allow the system to prevent attacks by multiple browser requests.". The reference Lin teaches "A filter 106

operates to selectively block session establishment packets 108 from being provided to the target 104. In particular, an abnormally high number of session establishment attempts is usually an indication that a denial of service (DoS) attack is occurring. The filter 106 records the total number of existing sessions and measures the rate of session requests of each stream. A "stream" is a data traffic flow between a particular source and a specific target.", col. 2, lines 10-16 ("to allow the system to prevent attacks by multiple browser requests."). As it is evident from the depiction of the Lin's filter in Fig. 1, the filter itself affords its implementation anywhere in a given system. Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to enhance Bandhole's webserver and its account manager, Fig.3, element 329 (the application server interface) by adding Lin's filter such that the denial of service attacks can be handled without entirely blocking all new session connection requests. Again, this would have been obvious because it allows rather than denying all new session requests or denying no new session requests (and, albeit, dropping then-pending session requests), new session requests are selectively passed to the device.

Referring to claim 17,

The reference Bandhole teaches a method according to Claim 15, further comprising: routing the incoming browser request to one of a plurality of webservers (Figs 2 and 3) ;

screening the browser requests by retrieving browser request privilege information from the state table and determining whether the browser request is authorized to be sent to an application server to prevent unauthorized access to an application server with browser requests: receiving the request by a first webserver; and

transferring identification information related to other webservers to the application server. (page 6, para.[0049], Fig.3, elements 331 and 329, page 6, para. [0054]-[0056]).

Referring to claim 18,

The reference Bandhole teaches a method according to Claim 15, wherein the step of facilitating communication between the application server and the webserver includes facilitating a session of communication between the application server and the webserver and to facilitate access only by authorized browser requests to prevent attack on an application server b browse nests. (Fig.3, elements 329 and 331, page 6, para.[0049] and [0054]-[0056])

Referring to claim 19,

The reference Bandhole teaches a method according to Claire 15, wherein facilitating communication between the browser and the application server with the webserver is done in response to receiving a signal from the application server indicating that it is ready to receive a browser request and in response to preauthorization of access of a browser request, to an application server by a webserver by accessing the state table to determine the browser request privileges. (Fig.3, elements 329 and 331, page 6, para.[0049] and [0054]-[0056], [0052], "That is, each of the managers need not reside in a single application server 311, but rather might be operably disposed over two or more machines.")

Referring to claim 21,

The reference Bandhole teaches a method according to Claim 15, wherein the step of facilitating communication between the application server and the webserver includes

facilitating a session of communication between the application server and the webserver in response to receiving signal from the application server indicating that it is ready to receive a browser request and in response to preauthorization of access of a browser request to an application server by a webserver by accessing the state table to determine the browser request privileges. (Fig.3, elements 329 and 331, page 6, para.[0049] and [0054]-[0056], [0052], "That is, each of the managers need not reside in a single application server 311, but rather might be operably disposed over two or more machines.")

Conclusion

Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ashok B. Patel whose telephone number is (571) 272-3972. The examiner can normally be reached on 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John A Follansbee can be reached on (571) 272-3964. The fax phone

number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abp
***

JOHN [illegible] LANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100